ABELSCHE KÖRPER ALS KREISTEILUNGSKÖRPER

INAUGURAL-DISSERTATION
ZUR ERLANGUNG DER DOKTORWÜRDE
GENEHMIGT VON DER PHILOSOPHISCHEN
FAKULTÄT DER FRIEDRICH-WILHELMS-
UNIVERSITÄT ZU BERLIN

VON

FRIEDRICH STEINBACHER
AUS BERLIN.

ACAD.
LUGD.BAT.
BIBL.

TAG DER PROMOTION: 14. DEZEMBER 1910.

BERLIN
DRUCK VON GEORG REIMER
1910

REFERENTEN: PROF. DR. FROBENIUS
PROF. DR. H. A. SCHWARZ.

Sonderabdruck aus dem Journal für die
reine und angewandte Mathematik Bd. 139.
Herausgegeben von K. Hensel.
Verlag von Georg Reimer, Berlin.

Daß jeder *Abel*sche Körper ein Kreisteilungskörper ist, hat *Kronecker* entdeckt und nach seinen Andeutungen Herr *Weber* bewiesen (Acta Math., Bd. 8). Dieser Beweis ist in vereinfachter Form im Lehrbuch der Algebra desselben Verfassers (Bd. 2) dargestellt. Einen zweiten Beweis teilte Herr *Hilbert* in den Nachrichten der Kgl. Gesellschaft der Wissenschaften zu Göttingen (Math.-phys. Kl., 1896) mit, den er in kürzerer Form in Bd. 4 des Jahresberichtes der Deutschen Mathematiker-Vereinigung wiedergab. Herr *Mertens* hat schließlich in einer Untersuchung über zyklische Körper in Bd. 131 dieses Journals einen dritten Beweis niedergelegt, worauf es Herrn *Weber* gelang, in Bd. 132 desselben Journals seinem früheren Beweise eine sehr viel kürzere Form zu geben. Das geschah besonders durch die Einführung der vollständigen Induktion, die zuerst Herr *Hilbert* für unsern Satz benutzt hatte.

Jeder Beweis, der denselben Weg einschlagen will, zerfällt nun naturgemäß in zwei Teile. Zunächst ist zu zeigen, daß jeder zyklische Körper p-ten Grades, wo p irgendeine rationale Primzahl ist, mit einem Kreisteilungskörper identisch ist. Daraus ist dann zu folgern, daß auch jeder *Abel*sche Körper höheren Grades ein Kreisteilungskörper ist. In beiden Teilen des Beweises ist es vorteilhaft, sich auf die Untersuchungen zu beziehen, die Herr *Hilbert* über die Zerlegung einer Primzahl in einem beliebigen Körper angestellt hat. Es ist besonders der Begriff der Trägheitsgruppe eines Primideals, der hier von fundamentaler Bedeutung wird und durch den sich die Beweisführung wesentlich vereinfachen läßt, wie in der vorliegenden Arbeit nachgewiesen werden soll.

Für den ersten Teil des Beweises stützt sich Herr *Hilbert* auf den Satz von *Minkowski*, daß außer dem Körper der rationalen Zahlen kein Körper mit der Diskriminante ± 1 möglich sei. Dieser Satz gehört zu

den schwierigsten der Zahlentheorie, ist aber für uns nicht in seiner Allgemeinheit nötig. Wir haben ihn nur für zyklische Körper des Grades p zu beweisen. Hier führt eine Konstruktion von *Kummer* zum Ziel, ähnlich der, die Herr *Hilbert* für den relativ-zyklischen Körper durchgeführt hat (Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 4, S. 271ff; im folgenden zitiert als *Hilbert*, B.). Einen solchen Beweis gebe ich im zweiten Abschnitt dieser Arbeit. Dieser Beweis ist auch sonst für unser Thema nicht ohne Interesse. Man kann aus ihm leicht schließen, daß ein zyklischer Körper p-ten Grades stets dann ein Kreisteilungskörper ist, wenn p nicht in seiner Diskriminante aufgeht.

Ist dagegen p in dieser Diskriminante enthalten, so reichen diese Schlüsse nicht aus. Der Fall, wo der *Abel*sche Körper ein zyklischer Körper p-ten Grades mit der Diskriminante p^a ist, bildet überhaupt den schwierigsten Teil des allgemeinen Satzes. Hier muß eine Beziehung zwischen dem zyklischen Körper und demjenigen Körper des Grades $p-1$ hergestellt werden, der von den p-ten Einheitswurzeln gebildet wird. Eine solche, algebraisch sowohl wie zahlentheoretisch wohl bekannte Beziehung wird durch die Resolventen von *Lagrange* gegeben. Sie definieren einen *Abel*schen Körper des Grades $p(p-1)$, der in allen Beweisen unseres Satzes eine wichtige Rolle spielt. Die Herren *Weber* und *Mertens* zeigen direkt, daß dieser Körper mit einem Kreisteilungskörper übereinstimmt, wobei sie sich auf *Kummer*s Untersuchungen über die arithmetischen Eigenschaften solcher Körper stützen. Herr *Hilbert* hat im Hinblick auf die Wichtigkeit dieser Untersuchungen derartige Körper als *Kummer*sche Körper bezeichnet. Er kann sich mit dem Beweise begnügen, daß nur ein einziger solcher Körper mit den verlangten Eigenschaften existiert. Wir werden auch diesen Beweis im Zusammenhang mit der *Kummer*schen Konstruktion einfacher gestalten können.

Die Theorie der algebraischen Zahlen wird im folgenden immer in dem Umfange vorausgesetzt, wie sie im 18. und 19. Abschnitt des zweiten Bandes von *Weber*s Algebra (2. Aufl.) dargestellt ist. Zunächst stelle ich eine Reihe dort bewiesener Sätze zusammen, indem ich ihnen die für unsere Zwecke nötige Formulierung gebe.

Die im 5. Abschnitt benutzten Sätze über das Verhältnis zwischen dem Produkt und dem größten gemeinsamen Teiler zweier Körper ver-

danke ich der Vorlesung, die Herr *Frobenius* über Algebra zu halten pflegt. Ihm bin ich auch für Rat und Anregung in bezug auf die übrigen Teile der Arbeit zu vielem Danke verpflichtet.

1. *Die Diskriminante Abelscher Körper.*

Es sei P ein *Abel*scher Körper n-ten Grades, $\mathfrak{G}=(G_0=E, G_1, G_2, \dots G_{n-1})$ seine Gruppe, $\omega_1, \omega_2, \dots \omega_n$ eine Basis der ganzen Zahlen dieses Körpers. Sind $t_1, t_2, \dots t_n$ unabhängige Variable, so heißt $\tau = t_1\omega_1 + t_2\omega_2 + \cdots + t_n\omega_n$ eine *Fundamentalform* oder *Basisform des Körpers*. Durch die Substitution G gehe τ über in τ_G.

Jede rationale Primzahl p zerfällt in P in e verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_e$, wo e auch gleich 1 sein kann, und es ist $p=(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_e)^g$. Es gibt in $\mathfrak{G}$ eine Untergruppe $\mathfrak{T}$ von der Ordnung g, $\mathfrak{T}=(T_0=E, T_1, T_2, \dots T_{g-1})$, so daß stets $\tau_T \equiv \tau \pmod{\mathfrak{p}_1}$ ist. Diese Gruppe nennt Herr *Hilbert* die *Trägheitsgruppe* von $\mathfrak{p}_1$. Die Primideale $\mathfrak{p}_2, \dots \mathfrak{p}_e$ haben ebenfalls Trägheitsgruppen; diese sind zu $\mathfrak{T}$ konjugiert und folglich, weil wir $\mathfrak{G}$ als eine *Abel*sche Gruppe angenommen haben, mit $\mathfrak{T}$ identisch. Wir wollen deshalb im folgenden $\mathfrak{T}$ die Trägheitsgruppe von p nennen. Die Ordnung von $\mathfrak{T}$ ist $p'p^\alpha$, wo p' ein Teiler von p^f-1 ist, wenn f aus der Gleichung $n=efg$ bestimmt wird. Die Zahl p' ist deshalb nicht mehr durch p teilbar. In $\mathfrak{T}$ ist nach einem bekannten Satz von *Sylow* eine Untergruppe $\mathfrak{V}=(V_0=E, V_1, V_2, \dots V_{p^\alpha-1})$ von der Ordnung p^α enthalten. Sie hat die Eigenschaft, daß $\tau_V \equiv \tau \pmod{\mathfrak{p}_\lambda^2}$ ist und heißt die Verzweigungsgruppe von $\mathfrak{p}_\lambda$ oder von p. Für unsere Zwecke ist die Tatsache von größter Wichtigkeit, daß die Gruppe $\mathfrak{T}/\mathfrak{V}$ eine zyklische Gruppe von der Ordnung p' ist.

Die algebraische Form $f(\tau)=(\tau-\tau_{G_1})(\tau-\tau_{G_2})\cdots(\tau-\tau_{G_{n-1}})$ ist eine ganze rationale Funktion von $t_1, t_2, \dots t_n$ mit Koeffizienten, die ganze Zahlen in P sind. Die Norm von $f(\tau)$, $Nf(\tau)$, ist eine ebensolche Funktion mit ganzen rationalen Koeffizienten, deren größter gemeinschaftlicher Teiler die Diskriminante Δ von P ist. Wir sagen im Anschluß an *Kronecker*, daß dann $Nf(\tau)$ äquivalent $(\backsim)\Delta$ ist. Hat p eine von E verschiedene Trägheitsgruppe, so sieht man, daß mindestens einer der Faktoren von $f(\tau)$ durch $\mathfrak{p}_\lambda$ teilbar ist, daß also p in Δ aufgeht. Nur dieser Fall hat für uns Interesse, und wir reden von einer Trägheitsgruppe nur dann, wenn sie von E verschieden ist.

Ist nun $\mathfrak{H} = (H_0 = E, H_1, H_2, \dots H_{h-1})$ eine Untergruppe von $\mathfrak{G}$ von der Ordnung h, so gehört im Sinne der Algebra zu $\mathfrak{H}$ ein Teiler P_1 von P vom Grade $i = \frac{n}{h}$ mit der Diskriminante Δ_1, und es ist $\mathfrak{G} = \mathfrak{H} + \mathfrak{H}G_1 + \mathfrak{H}G_2 + \cdots + \mathfrak{H}G_{i-1}$, wo $G_1, G_2, \dots G_{i-1}$ passend gewählte Elemente von $\mathfrak{G}$ sind. Wir können dann schreiben:

$$\begin{aligned} f(\tau) = \quad & (\tau - \tau_{H_1}) \quad (\tau - \tau_{H_2}) \cdots \quad (\tau - \tau_{H_{h-1}}) \\ (\tau - \tau_{G_1}) \quad & (\tau - \tau_{H_1 G_1}) \quad (\tau - \tau_{H_2 G_1}) \cdots \quad (\tau - \tau_{H_{h-1} G_1}) \\ & \cdots \cdots \cdots \cdots \cdots \\ & (\tau - \tau_{G_{i-1}})(\tau - \tau_{H_1 G_{i-1}})(\tau - \tau_{H_2 G_{i-1}}) \cdots (\tau - \tau_{H_{h-1} G_{i-1}}). \end{aligned}$$

Bezeichnen wir das Produkt in der ersten Zeile mit $g(\tau)$, das Übrige mit $h(\tau)$, so ist $f(\tau) = g(\tau) h(\tau)$, und es wird $N h(\tau) \backsim \Delta_1^h$ (*Hilbert*, B. § 16, *Weber* Bd. II, § 177).

Ist $\mathfrak{H}$ die Trägheitsgruppe von p, so sind nur die Faktoren von $g(\tau)$ durch Primideale von p teilbar, nicht die von $h(\tau)$. P_1 heißt dann der Trägheitskörper von p, und wir haben den Satz, daß die Diskriminante des Trägheitskörpers von p nicht durch p teilbar ist. Dies genügt für das Folgende. Es ergibt sich aber aus der obigen Formel der noch schärfere Satz:

In einem Abelschen Körper P ist der Trägheitskörper von p derjenige Teiler von P, der die größte durch p nicht teilbare Diskriminante hat.

Hat daher P die Beschaffenheit, daß jede Diskriminante Δ_1 durch p teilbar ist, so ist der Trägheitskörper von p der Körper der rationalen Zahlen, und $\mathfrak{G}$ ist selber die Trägheitsgruppe von p.

2. *Es gibt keinen zyklischen Körper mit der Diskriminante* ± 1.

Es sei A ein zyklischer Körper vom Primzahlgrade p, ferner $\omega_1, \omega_2, \dots \omega_p$ eine Basis seiner ganzen Zahlen. Seine Gruppe $\mathfrak{S}$ besteht aus den Potenzen einer einzigen Substitution S von der Ordnung p. Wir machen hier mit Vorteil von einer bequemen Schreibweise Gebrauch, die Herr *Hilbert* eingeführt hat (B., S. 271), indem wir $\omega_{S^\beta}^{\alpha} = \omega^{\alpha S^\beta}$ setzen. Dann ist $\omega^{S^p} = \omega^E = \omega$ oder $\omega^{S^p - 1} = 1$.

Zunächst sei $p > 2$. Aus der allgemeinen Theorie der algebraischen Zahlen (vgl. *Dirichlet-Dedekind*, Vorlesungen über Zahlentheorie, 4. Aufl. § 183) brauchen wir nur den Satz, daß es in A eine von ± 1 verschiedene Einheit gibt.

Von *Kummer* rührt eine interessante Verallgemeinerung der Resolventen von *Lagrange* her (Zwei neue Beweise der allgemeinen Reziprozitätsgesetze usw., Abh. der Akad. der Wiss. zu Berlin 1861, auch dieses Journal Bd. 100), die Herr *Hilbert* (B., S. 272) noch weiter ausgedehnt hat. Ich brauche sie hier in folgender Form: Für die oben genannte Einheit ε und für irgendeinen Wert von $\varkappa$ sei:

$$(1.) \qquad \alpha = \omega_\varkappa + \omega_\varkappa^S \varepsilon + \omega_\varkappa^{S^2} \varepsilon \varepsilon^S + \cdots + \omega_\varkappa^{S^{p-1}} \varepsilon \varepsilon^S \varepsilon^{S^2} \cdots \varepsilon^{S^{p-2}};$$

dann folgt daraus

$$(2.) \qquad \alpha = \varepsilon \alpha^S,$$

weil $\varepsilon \varepsilon^S \varepsilon^{S^2} \ldots \varepsilon^{S^{p-1}} = 1$ ist. Die p Größen α, die sich aus (1.) ergeben, können nicht sämtlich Null sein, denn in diesem Falle würde (1.) ein System von p homogenen linearen Gleichungen für die nicht verschwindenden Größen $1, \varepsilon, \varepsilon\varepsilon^S, \ldots$ darstellen, dessen Determinante gleich der Quadratwurzel aus der Diskriminante von A ist, also ebenfalls nicht verschwindet. In (2.) darf ich demnach α von Null verschieden annehmen. Es ist eine algebraische Zahl in A, die nicht selber rational sein kann, wohl aber durch eine ganze rationale Zahl teilbar sein könnte. Ein solcher Faktor würde dann auch in α^S vorkommen und kann aus (2.) fortgelassen werden. Das soll im folgenden immer geschehen sein. Jeder Einheit ε entspricht mindestens eine solche Größe α; wir können schreiben: $\varepsilon = \alpha^{1-S}$. Nun kann α ebenfalls eine Einheit sein; es gilt jedoch der Satz:

Es gibt in A solche Einheiten ε, für welche die Größe α keine Einheit ist.

Gibt es nämlich solche Einheiten nicht, so ist etwa $\varepsilon = \varepsilon_1^{1-S}$; ebenso aber wird $\varepsilon_1 = \varepsilon_2^{1-S}$ usw., wo die $\varepsilon_\varkappa$ stets Einheiten sind. Die Größe ε läßt sich durch jede dieser unendlich vielen Größen $\varepsilon_\varkappa$ ausdrücken, und es wird $\varepsilon = \varepsilon_1^{1-S} = \varepsilon_2^{(1-S)^2} = \cdots = \varepsilon_\varkappa^{(1-S)^\varkappa}$. Insbesondere ist $\varepsilon = \varepsilon_p^{(1-S)^p}$. Wird der Exponent nach dem binomischen Lehrsatz entwickelt, so kommt rechts der Faktor $\varepsilon^{1-S^p} = 1$ vor. Die übrigen Potenzen von S haben alle durch p teilbare Koeffizienten; das heißt aber, daß ε die p-te Potenz einer anderen Einheit in A ist, oder, daß auch $\sqrt[p]{\varepsilon}$ eine Einheit in A ist. Diese nenne ich ε'. Von ε' ausgehend komme ich zu einer neuen Einheit $\varepsilon'' = \sqrt[p]{\varepsilon'}$ usw. Dieser Prozeß kann aber nicht unendlich viele Male fortgesetzt werden; denn sei G eine Größe größer als 1, unterhalb deren ε und die ihm konjugierten

Größen alle dem absoluten Werte nach liegen, so gilt dasselbe auch von $\varepsilon', \varepsilon'', \ldots$. Nun gibt es aber nur eine endliche Anzahl von Gleichungen n-ten Grades, in denen der Koeffizient der höchsten Potenz gleich 1 ist, die übrigen rationale ganze Zahlen sind und deren Wurzeln dem absoluten Betrage nach kleiner als G sind.

Unser Verfahren führt folglich nach einer endlichen Anzahl von Schritten zu einer Einheit ε, für die das zugehörige α keine Einheit mehr ist.

Ist dagegen $p=2$, so genügt es, $\varepsilon=-1$ zu nehmen. Ist ω eine den Körper bestimmende ganze Zahl, so setzen wir $\alpha=\omega-\omega^S$, also $\alpha^S=\omega^S-\omega$ und folglich $\alpha=-\alpha^S$. Ist α nach Entfernung der rationalen Faktoren keine Einheit, so ist unser Ziel erreicht; wird dagegen $\varepsilon_1=-\varepsilon_1^S$, so ergibt sich wegen $\varepsilon_1\varepsilon_1^S=\pm 1$:

$$\varepsilon_1^2=\pm 1,$$

und da wegen $\varepsilon_1=-\varepsilon_1^S$ das Zeichen $+$ nicht gilt, so folgt $\varepsilon_1=i$. Der Körper $P(i)$ hat aber die Diskriminante -4.

Die Größe α untersuchen wir nun in bezug auf die in ihr enthaltenen Primideale. Es sei q eine rationale Primzahl, die mit α einen Teiler gemeinsam habe. Im ersten Abschnitt ist ausgeführt worden, daß zu q drei Zahlen e,f,g gehören, so daß $efg=n$ ist, die die Zerlegbarkeit von q bestimmen. Hier ist $n=p$, also müssen stets zwei dieser Größen gleich 1 sein, die dritte ist p. Wenn $f=p$ ist, so bleibt q auch in $\mathcal{A}$ eine Primzahl; sie kann nach unserer Voraussetzung in α nicht aufgehen.

Ist $e=p$, so wird $q=\mathfrak{q}\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_{p-1}$. Dann sei α etwa durch $\mathfrak{q}$ teilbar. Durch S gehe $\mathfrak{q}$ in $\mathfrak{q}_1$ über, durch S^2 in $\mathfrak{q}_2$ usw.; dann ist α^S durch $\mathfrak{q}_1$ teilbar, vermöge der Gleichung (2.), demnach auch α; hieraus folgt wieder, daß α^S durch $\mathfrak{q}_2$ teilbar ist, also auch α; es zeigt sich schließlich, daß α durch $\mathfrak{q}\mathfrak{q}_1\cdots\mathfrak{q}_{p-1}=q$ teilbar ist, was wir ausgeschlossen hatten.

In α sind demnach nur Primteiler solcher Primzahlen enthalten, für die $g=p$ ist. Ist q eine Primzahl dieser Art, so ist $q=\mathfrak{q}^p$. Daher ist q in der Diskriminante von $\mathcal{A}$ enthalten. Da jeder *Abel*sche Körper einen zyklischen Körper $\mathcal{A}$ enthält und die Diskriminante eines Körpers durch die Diskriminante jedes Teilers teilbar ist, so haben wir den allgemeineren Satz:

In der Diskriminante eines Abelschen Körpers ist mindestens eine Primzahl enthalten.

Von der Primzahl q, die mit α einen Teiler gemeinsam hat, gilt ein wichtiger Satz, zu dessen Ableitung wir nun übergehen.

3. *Zyklische Körper, deren Diskriminante nur eine einzige Primzahl enthält.*

Wir gehen wieder von dem im vorigen Abschnitt behandelten Körper p-ten Grades aus und nehmen an, daß seine Diskriminante eine Potenz einer rationalen Primzahl q ist, wo q nicht von p verschieden zu sein braucht. Es wird $q=\mathfrak{q}^p$, und die Zahl α, welche der Bedingung $\alpha=\varepsilon\alpha^S$ genügt, enthält nur den Idealteiler $\mathfrak{q}$, ist also etwa gleich $\mathfrak{q}^a$, wo a zwischen 1 und $p-1$ liegt. Genügt dann b der Kongruenz $ab\equiv 1 \pmod p$, so ist $\alpha^b=q^c\alpha_1$, $\alpha^{bS}=q^c\alpha_1^S$, $\alpha^b=\varepsilon^b\alpha^{bS}$, folglich $\alpha_1=\varepsilon^b\alpha_1^S$. Hier ist α_1 nur durch $\mathfrak{q}$ teilbar und durch keine höhere Potenz von $\mathfrak{q}$. Im folgenden benutzen wir immer nur eine solche Größe α_1, die wir wieder mit α bezeichnen. Schreiben wir statt ε^b wieder ε, so haben wir auch hier $\alpha=\varepsilon\alpha^S$, und es ist $\alpha^p=\eta q$, wo η eine Einheit ist.

Von jetzt ab trennen wir zweckmäßig die beiden Fälle, wo q von p verschieden ist und wo $q=p$ ist. Der erste läßt sich im Hinblick auf unser Thema leicht und erschöpfend behandeln.

Es zeigt sich zunächst, daß die Primzahl q nicht beliebig sein kann. Hier gilt ein Satz, den wir gleich in seiner allgemeinsten Form aussprechen und beweisen:

Hat ein zyklischer Körper des Grades p^a die Eigenschaft, daß der in ihm enthaltene Teiler p-ten Grades eine durch q teilbare Diskriminante hat, so ist $q-1$ durch p^a teilbar.

Da unser Körper als zyklischer nur einen einzigen Teiler p-ten Grades hat, so geht dieser auch in allen übrigen Teilern auf. Sämtliche Diskriminanten sind daher durch q teilbar. Nach den Ausführungen des ersten Abschnitts ist deshalb der Körper der rationalen Zahlen Trägheitskörper von q, die Gruppe des gegebenen Körpers selber die Trägheitsgruppe, $g=p^a$, $f=1$. Es war stets $g=q'q^b$, wo q' ein Divisor von $q-1$ ist. Wir haben folglich $p^a=q'q^b$, daraus ergibt sich $b=0$, und p^a ist deshalb in $q-1$ enthalten. Das dürfte der kürzeste und natürlichste Beweis des wichtigen Satzes sein (vgl. z. B. *Hilbert*, B., S. 342).

Wir betrachten nun einen zyklischen Körper des Grades p^a, dessen Diskriminante nur durch q teilbar ist. Es ist also $q-1$ durch p^a teilbar. Einen solchen Körper finden wir unter den Kreisteilungskörpern; denn aus der Gleichung $x^q=1$ entspringt ein Körper des Grades $q-1$, der selber zyklisch ist und deshalb einen zyklischen Teiler des Grades p^a enthält. Diesen Körper nennen wir P. Seine Diskriminante ist eine Potenz von q. Ich behaupte, daß es einen zweiten Körper dieser Art nicht gibt: Wäre P_1 ein zweiter Körper, so wäre das Produkt von P und P_1 ein *Abel*scher Körper des Grades p^b $(b>a)$, dessen Diskriminante gleichfalls eine Potenz von q sein würde. Dieser Körper wäre nicht zyklisch, denn sonst könnte er nur einen Teiler des Grades p^a haben, da eine zyklische Gruppe der Ordnung p^b nur einen Teiler der Ordnung p^{b-a} hat. Seine Gruppe wäre die Trägheitsgruppe von q. Da ihre Ordnung nicht durch q teilbar ist, so wäre $\mathfrak{B}=E$. Es ist aber stets $\mathfrak{T}/\mathfrak{B}$ zyklisch, also müßte die Gruppe zyklisch sein, was ein Widerspruch ist. Damit ist bereits die Identität einer ganzen Klasse von zyklischen Körpern mit Kreisteilungskörpern nachgewiesen.

4. *Der zyklische Körper p-ten Grades mit der Diskriminante p^a.*

Es bleibt der zweite und schwierigere Fall zu erledigen, wo die Diskriminante des zyklischen Körpers p-ten Grades nur die Primzahl p enthält. Wenn wir an den oben dargelegten Gedankengang anknüpfen, so werden wir uns Kreisteilungskörper verschaffen müssen, die mit den gegebenen zyklischen Körpern zu vergleichen sind.

Ist $p=2$, so ist der aus $\frac{x^{2^a}-1}{x^{2^{a-1}}-1}=x^{2^{a-1}}+1=0$ entspringende Kreisteilungskörper kein zyklischer. Er enthält, wie aus der Form der Gleichung ersichtlich ist, die Zahl i, und in seiner Gruppe ist daher eine Substitution A der Ordnung 2, die i in $-i$ überführt. Der dazu gehörige Teiler $\mathcal{A}$ enthält also nur reelle Zahlen; er ist zyklisch vom Grade 2^{a-2}. Dazu kommt als zweiter Teiler der rein-imaginäre quadratische Körper $P(i)$. Nehmen wir den einfachsten Fall $a=3$, so enthält der Körper vierten Grades, der aus $x^4+1=0$ entsteht, den reellen Teiler $\mathcal{A}=P(\sqrt{2})$, ferner $P(i)$ und deshalb auch $P(i\sqrt{2})$. Alle Diskriminanten sind Potenzen von 2. Aus den Betrachtungen des zweiten Abschnittes folgt sofort, daß es außer den drei genannten keinen Körper zweiten Grades gibt, dessen Diskriminante dieselbe Eigenschaft hat.

Betrachten wir nun wieder den Körper des Grades 2^{a-1}, so besteht seine Gruppe aus Substitutionen von der Form $A^\alpha B^\beta$, wo A die Ordnung 2, B die Ordnung 2^{a-2} hat. Zu A sollte $\mathcal{A}$ gehören, zu B gehört dann $P(i)$. Die Gruppe kann aber auch in die Form $C^\gamma D^\delta$ gebracht werden, wo $C=AB^{2^{a-3}}$ und $D=AB$ ist. Da C die Ordnung 2 hat, so gehört zu $\mathfrak{C}=(C^\gamma)$ ein zweiter zyklischer Körper B des Grades 2^{a-2}. Dieser Körper hat mit $\mathcal{A}$ einen Teiler des Grades 2^{a-3} gemeinsam. Zu $\mathfrak{D}=(D^\delta)$ gehört demnach der Körper $P(i\sqrt{2})$, und B besteht nicht nur aus reellen Zahlen, aber alle in ihm enthaltenen reellen Zahlen bilden einen Teiler des Grades 2^{a-3}, der auch in $\mathcal{A}$ enthalten ist. Gäbe es außer $\mathcal{A}$ und B noch einen weiteren zyklischen Körper des Grades 2^{a-2} mit einer nur durch 2 teilbaren Diskriminante, so ist er entweder reell oder imaginär. Im letzteren Falle enthält er außer jeder Zahl $a+bi$ auch die konjugierte $a-bi$; die Substitution seiner Gruppe, welche die eine in die andere überführt, ist von der Ordnung 2 und gehört zu einem reellen Körper des Grades 2^{a-3}. So haben wir aus dieser Betrachtung folgendes Resultat gewonnen:

Es gibt drei zyklische Körper 2-ten Grades mit nur durch 2 teilbarer Diskriminante; es sind der reelle Körper $P(\sqrt{2})$ und die imaginären $P(i)$ und $P(i\sqrt{2})$. Das sind Kreisteilungskörper. Hat dagegen der zyklische Körper den Grad 2^a, wo $a>1$ ist, so besitzt er einen reellen Teiler mindestens vom Grade 2^{a-1}, enthält also jedenfalls den Körper $P(\sqrt{2})$.

Von nun an sei $p>2$ und $\mathcal{A}$ ein zyklischer Körper p-ten Grades mit der Diskriminante p^a. In ihm ist $p=\mathfrak{p}^p$, wo $\mathfrak{p}$ das durch die oben erhaltene Zahl α definierte Hauptideal ist. Die Gruppe $\mathfrak{A}$ von $\mathcal{A}$ ist die Trägheitsgruppe von p, und da ihre Ordnung gleich p ist, auch die Verzweigungsgruppe von p. Demnach ist $\tau\equiv\tau^A \pmod{\alpha^2}$. Jeder Faktor von $f(\tau)$ ist mindestens durch α^2 teilbar, und $Nf(\tau)$ oder Δ_p mindestens durch $p^{2(p-1)}$. Es wird sich später ergeben, daß Δ_p genau gleich $p^{2(p-1)}$ ist (vgl. unten (4.)).

Ferner sei B der Körper der p-ten Einheitswurzeln vom Grade $p-1$. Wir können in derselben Weise schließen, daß seine Diskriminante $\Delta_{p-1}=p^{p-2}$ ist.

Aus $\mathcal{A}$ und B bilden wir nun jenen *Abel*schen (sogar zyklischen) Körper P des Grades $p(p-1)$, der seit den Zeiten von *Lagrange* in der Algebra und der Zahlentheorie eine so wichtige Rolle gespielt hat. Seine

Gruppe $\mathfrak{G}$ ist das Produkt aus einer Gruppe $\mathfrak{S}=(S^x)$ von der Ordnung p und einer Gruppe $\mathfrak{R}=(R^\lambda)$ der Ordnung $p-1$, wo A zu $\mathfrak{R}$ und B zu $\mathfrak{S}$ gehört. In A war p genau durch α^p teilbar. Ist ϱ eine p-te Einheitswurzel und bezeichnen wir $1-\varrho$ mit β, so ist in B die Primzahl p gleich der $(p-1)$-ten Potenz des durch β bestimmten Hauptideals. Für P ist $\mathfrak{G}$ die Trägheitsgruppe von p, also $p=\mathfrak{p}^{p(p-1)}$, daher ist $\alpha=\mathfrak{p}^{p-1}$ und $\beta=\mathfrak{p}^p$, und $\mathfrak{p}$ ist das durch $\frac{\beta}{\alpha}$ bestimmte Hauptideal.

Wir bestimmen die Diskriminante Δ von P. Zu dem Zwecke bilden wir $f(\tau)$ in doppelter Weise nach den Vorschriften des ersten Abschnitts. Einmal sei die erste Zeile $(\tau-\tau^S)(\tau-\tau^{S^2})\cdots(\tau-\tau^{S^{p-1}})$. Die übrigen Zeilen bilden, wenn wir zu $Nf(\tau)$ übergehen, $\Delta_{p-1}^p=p^{p(p-2)}$. $\mathfrak{S}$ ist die Verzweigungsgruppe von p, also ist $\tau-\tau^{S^x}$ durch $\mathfrak{p}^a$ teilbar, wo $a\geqq 2$ ist. Gehen wir auch hier zur Norm über, so wird $\Delta=p^{a(p-1)+p(p-2)}$. Andererseits können wir $f(\tau)$ auch anfangen lassen mit $(\tau-\tau^R)(\tau-\tau^{R^2})\cdots(\tau-\tau^{R^{p-2}})$. Aus den übrigen Zeilen ergibt sich $\Delta_p^{p-1}\geqq p^{2(p-1)^2}$. Von den Faktoren $\tau-\tau^{R^\lambda}$ ist jeder nur durch $\mathfrak{p}$ teilbar, demnach wird jetzt $\Delta\geqq p^{2(p-1)^2+p-2}$. Vergleichen wir die erhaltenen Werte, so muß $a(p-1)+p(p-2)\geqq 2(p-1)^2+p-2$ sein oder $a\geqq p$. Ist demnach μ eine beliebige Zahl in P, so haben wir das später wichtig werdende Resultat, daß $\mu-\mu^S$ durch $\mathfrak{p}^p$ teilbar ist. Hiermit stellen wir die Tatsache zusammen, daß durch S die Zahl α in α^S übergeht, wo $\alpha=\varepsilon\alpha^S$ ist, so daß $\alpha-\alpha^S=\alpha^S(\varepsilon-1)$ durch α^2 teilbar ist, also $\varepsilon-1$ durch α oder $\mathfrak{p}^{p-1}$.

Für den Körper A bilden wir die Resolventen von *Lagrange*. Ist ω eine primitive Zahl von A, so sei

$$\lambda=\omega+\varrho\,\omega^S+\varrho^2\omega^{S^2}+\cdots+\varrho^{p-1}\omega^{S^{p-1}}; \tag{1.}$$

daraus folgt dann

$$\lambda=\varrho\,\lambda^S, \tag{2.}$$

und daraus

$$\lambda^p=\lambda^{pS}. \tag{3.}$$

λ ist eine von Null verschiedene Größe, die nach (2.) keine Zahl von B ist, dagegen ist nach (3.) λ^p eine solche Zahl, die wir $\varphi(\varrho)$ nennen wollen. Wir können also setzen: $\lambda=\sqrt[p]{\varphi(\varrho)}$. Ist λ durch eine Zahl von B teilbar, so lassen wir einen solchen Faktor weg. (Es kann z. B. leicht gezeigt werden, daß der Faktor β stets in λ enthalten ist.)

Die Substitution R kann so gewählt werden, daß sie ϱ in ϱ^2 überführt; aus $\lambda = \sqrt[p]{\varphi(\varrho)}$ soll dabei $\lambda' = \sqrt[p]{\varphi(\varrho^2)}$ werden. Es folgt dann aus (2.):

$$\lambda' = \varrho^2 (\lambda')^S.$$

Ferner ist $(\lambda^{p-2}\lambda')^S = \lambda^{p-2}\lambda'$ und folglich eine Zahl von B. Dieses Resultat kann benutzt werden, der Zahl λ eine besonders vorteilhafte Eigenschaft zu verschaffen. λ sollte nicht durch β teilbar sein; es ist aber möglich, daß λ noch durch $\mathfrak{p}$ teilbar ist. Ist nun $\lambda = \sqrt[p]{\varphi(\varrho)}$ genau durch $\mathfrak{p}^b$ teilbar $(b < p)$, so ist auch $\lambda' = \sqrt[p]{\varphi(\varrho^2)}$ durch $\mathfrak{p}^b$ teilbar und das Produkt $(\lambda^{p-2}\lambda')\lambda$ genau durch $\mathfrak{p}^{bp}$ oder β^b. Dieses Produkt kann keine Zahl in B sein, denn in der Klammer steht eine solche Zahl, und dann würde auch λ in B liegen, was ausgeschlossen ist. Dividieren wir die so erhaltene Größe durch β^b, so erhalten wir eine neue Größe λ, die nicht durch $\mathfrak{p}$ teilbar ist und der Bedingung (2.) genügt. Eine solche Größe λ legen wir der weiteren Untersuchung zugrunde.

Die Gleichung $\frac{x^{p^a}-1}{x^{p^{a-1}}-1} = 0$ liefert uns einen zyklischen Kreisteilungskörper des Grades $p^{a-1}(p-1)$, der einen zyklischen Teiler des Grades p^{a-1} enthält. Die Diskriminanten sind sämtlich Potenzen von p. Ist insbesondere $a = 2$, so ist $\frac{x^{p^2}-1}{x^p-1} = 0$ die Gleichung des Körpers P, der aus B und dem Kreisteilungskörper A_p besteht, den wir mit A vergleichen wollen. Setzen wir $x^p = y$, so können wir die Gleichung von P schreiben: $\frac{y^p-1}{y-1} = y^{p-1} + y^{p-2} + \cdots + y + 1 = (y-\varrho)(y-\varrho^2)\cdots(y-\varrho^{p-1})$. Daraus ergibt sich z. B. $x = \sqrt[p]{\varrho^a}$, und jede dieser Größen kann für λ gewählt werden. Diese λ sind sämtlich Einheiten; aus Sätzen, die *Kummer* bewiesen hat (vgl. *Weber*, Bd. II, S. 751), läßt sich folgern, daß das mit den eben dargelegten Eigenschaften von λ in ursächlichem Zusammenhang steht. Das ist der Weg, auf dem Herr *Weber* seinen Beweis führt; auch Herr *Mertens* benutzt diese *Kummer*schen Sätze.

Gehört nun λ wieder zu A, so ist $\lambda \equiv a \pmod{\mathfrak{p}}$, wo a eine ganze rationale Zahl ist, denn $\mathfrak{p}$ ist ein Primideal ersten Grades. Demnach ist $\lambda - a$ teilbar durch $\mathfrak{p}$, oder weil $\mathfrak{p}$ das durch $\frac{\beta}{a}$ bestimmte Hauptideal ist, $\lambda - a = \mu\frac{\beta}{a}$; hier ist μ eine ganze Zahl in P. Wenden wir darauf S an, so ergibt sich

$$\lambda^S - a = \mu^S \frac{\beta}{\alpha^S} \quad \text{oder} \quad \varrho^{-1}\lambda - a = \mu^S \frac{\beta^S}{\alpha}.$$

Aus der ersten und dritten Gleichung folgt

$$\alpha\lambda = \varrho(\varepsilon(\mu^S - \mu) - \mu(1-\varepsilon)) \text{ oder}$$

$$\varrho\mu(1-\varepsilon) = -\alpha\lambda + \varrho\varepsilon(\mu^S - \mu). \tag{4.}$$

Die rechte Seite ist hier genau durch $\mathfrak{p}^{p-1}$ teilbar, also auch die linke; folglich ist μ nicht mehr durch $\mathfrak{p}$ teilbar. Betrachten wir statt λ die zugehörige Zahl φ, so folgt aus $(\lambda - a)^p \equiv \lambda^p - a^p \pmod{p}$ wegen $\lambda^p = \varphi$ und $a^p \equiv a \pmod{p}$, daß $\varphi - a$ durch β, aber nicht durch β^2 teilbar ist.

Das ist aber hinreichend, um zu zeigen, daß nur ein einziger Körper A existiert, der demnach mit A_p identisch sein muß. Sind nämlich A und A_p verschieden, so ist ihr Produkt ein nicht zyklischer *Abel*scher Körper des Grades p^2. Ein solcher enthält, wie die Betrachtung seiner Gruppe zeigt, $p+1$ zyklische Körper $A, A_1, A_2, \ldots A_p$. Ihnen entsprechen die $p+1$ Zahlen $\varphi(\varrho)$, die wir mit $\varphi(\varrho), \varphi_1(\varrho), \ldots \varphi_p(\varrho)$ bezeichnen wollen. Wir hatten gezeigt, daß $\varphi_p(\varrho) = \varrho$ gewählt werden kann. Ist ψ eine beliebige Zahl von B, die nicht die p-te Potenz einer Zahl in B ist, so bestimmt die Größe $\sqrt[p]{\psi}$ einen Körper P des Grades $p(p-1)$, der B als Teiler enthält. Eine solche Größe ist für jedes k: $\varrho^k\varphi(\varrho)$. Der entsprechende Körper P ist ein Teiler des aus A, A_p und B entspringenden *Abel*schen Körpers; er ist also selber ein *Abel*scher Körper und muß mit dem Produkt aus irgendeinem A_k und B identisch sein. Es darf demnach $\varphi_k(\varrho) = \varrho^k\varphi(\varrho)$ gesetzt werden.

Nun ist $\varrho = 1-\beta$, $\varrho^2 = (1-\beta)^2 \equiv 1-2\beta \pmod{\beta^2}$ und allgemein $\varrho^k \equiv 1-k\beta \pmod{\beta^2}$. Ferner hat β die Eigenschaft, daß $1, \beta, \beta^2, \ldots \beta^{p-2}$ eine Basis der ganzen Zahlen von B bilden; folglich ist $\varphi \equiv a + a_1\beta \pmod{\beta^2}$, wo a_1 nach den obigen Ausführungen nicht durch p teilbar sein kann. Ist aber k so gewählt, daß $a_1 - ka \equiv 0 \pmod{p}$ ist, so ist $\varrho^k\varphi(\varrho) \equiv a \pmod{\beta^2}$, was wir als unmöglich nachgewiesen haben. Dieser Körper A_k existiert demnach nicht; da aber das Bestehen der $p+1$ verschiedenen Körper A aus dem Vorhandensein von zwei unter ihnen notwendig folgte, so ist diese Voraussetzung falsch, und wir haben bewiesen:

Es gibt nur einen zyklischen Körper des Grades p, dessen Diskriminante eine Potenz von p ist. Dieser ist ein Kreisteilungskörper.

Allgemein können wir unsere Resultate so zusammenfassen:

Die zyklischen Körper des Grades p^a, deren Diskriminante nur durch p teilbar ist, sind für $a=1$ Kreisteilungskörper; für $a>1$ enthalten sie einen Kreisteilungskörper p-ten Grades, der stets, auch im Falle $p=2$, reell ist.

Daß diese Körper selber Kreisteilungskörper sind, beweisen wir, indem wir gleichzeitig die ganze Untersuchung auf eine breitere Grundlage stellen.

5. *Produkte von zyklischen Körpern und Kreisteilungskörpern.*

Das Produkt zweier zyklischer Körper ist ein *Abel*scher Körper. Die Gruppe eines *Abel*schen Körpers hat die wichtige Eigenschaft, daß sie sich durch eine Basis darstellen läßt, d. h. es lassen sich Elemente $A, B, C, \ldots$ so auswählen, daß jedes Element sich auf eine und nur eine Weise in der Form $A^a B^b \cdots$ schreiben läßt, wo die $a, b, \ldots$ positive ganze Zahlen sind. Es läßt sich ferner stets so einrichten, daß die Ordnungen von $A, B, \ldots$ Primzahlpotenzen sind. Lassen wir ein Element aus dieser Basis fort, etwa A, so bilden die übrigen eine Gruppe, zu der ein zyklischer Körper gehört, dessen Grad mit der Ordnung von A übereinstimmt. Die so entstehenden zyklischen Körper sind teilerfremd, ihr Produkt ist der gegebene *Abel*sche Körper.

Auf diesen Sätzen baut sich die zahlentheoretische Behandlung *Abel*scher Körper auf. Wir machen davon für den Beweis eines algebraischen Hilfssatzes Gebrauch:

*Haben zwei zyklische Körper A_1 und A_2 des Grades p^a einen größten gemeinsamen Teiler A', so ist ihr Produkt A auch das Produkt von A_1 und einem teilerfremden Abelschen Körper niedrigeren Grades als p^a**).

Wenn zwei Normalkörper die Grade r_1 und r_2 haben, wenn ihr Produkt den Grad r und ihr größter gemeinsamer Teiler den Grad r' hat, so besteht die Gleichung $r_1 r_2 = r r'$. Für uns habe A' den Grad p^{a-b}, dann hat A den Grad p^{a+b}. A habe die Gruppe $\mathfrak{G}$, A_1 gehöre zu der Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$; da A_1 zyklisch ist, so gibt es eine Substitution G in $\mathfrak{G}$, so daß

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}G + \mathfrak{H}G^2 + \cdots + \mathfrak{H}G^{p^a-1}$$

wird. G hat demnach eine Ordnung $\geqq p^a$. Die Basis von $\mathfrak{G}$ enthält dann

*) Vgl. *Weber*, dieses Journal Bd. 132, S. 168 und Math. Ann. Bd. 67, S. 42.

ebenfalls ein Element A, dessen Ordnung $\geqq p^a$ ist, denn aus Elementen von niedrigerer Ordnung würde sich G nicht zusammensetzen lassen. Die übrigen Elemente der Basis bilden eine Gruppe der Ordnung $\leqq p^b$; dazu gehört ein zyklischer Körper des Grades $\geqq p^a$. Ist der Grad $> p^a$, so folgt aus der Gleichung $r_1 r_2 = rr'$, daß dieser Körper mit A_1 sowohl wie mit A_2 einen Teiler gemeinsam hat, dessen Grad mindestens p^{a-b+1} ist. Da er als zyklischer Körper nur einen Teiler dieses Grades haben kann, so wäre das auch ein gemeinsamer Teiler von A_1 und A_2, was unserer Voraussetzung widerspricht. Deshalb ist die Ordnung von G gleich p^a, und $\mathfrak{G}$ ist das Produkt der beiden teilerfremden Gruppen $\mathfrak{H}$ und $\mathfrak{G}_1 = (G^x)$. Zu $\mathfrak{G}_1$ gehört ein *Abel*scher Körper A_3 des Grades $p^b < p^a$. Damit ist der Hilfssatz bewiesen. Es kann auch leicht gezeigt werden, daß $\mathfrak{H}$ eine zyklische Gruppe, also A_3 ein zyklischer Körper ist.

Wir können jetzt die Untersuchung des vorigen Abschnittes zum Abschluß bringen: A_1 sei wieder der zyklische Kreisteilungskörper des Grades p^a, dessen Diskriminante eine Potenz von p ist (für $p = 2$ der reelle Körper dieser Art), A_2 ein anderer Körper desselben Grades mit derselben Eigenschaft. Wir haben gezeigt, daß beide mindestens einen Körper p-ten Grades gemeinsam haben. Der Körper A_3 hat dann einen Teiler p-ten Grades, dessen Diskriminante gleichfalls eine Potenz von p ist; er würde also zu A_1 nicht teilerfremd sein können, wenn $p > 2$ ist. Das widerspricht aber dem soeben bewiesenen Satz. Ist $p = 2$, so gilt entweder dasselbe, oder es ist A_3 einer der Körper $P(i)$ oder $P(i\sqrt{2})$. In jedem Falle aber ist bewiesen, daß alle diese Körper Kreisteilungskörper sind.

Dem ersten Hilfssatz stellen wir nun einen zweiten an die Seite. Es handelt sich immer um zyklische Körper des Grades p^a. Die Kreisteilungskörper sollen von nun an immer mit P bezeichnet werden. Damit alle Diskriminanten eines zyklischen Körpers vom Grade p^a durch eine Primzahl q teilbar sind, ist notwendig und hinreichend, daß die Diskriminante seines Teilers vom Grade p durch q teilbar ist. Solche Primzahl q will ich in Anlehnung an eine bekannte Bezeichnung eine totalkritische Primzahl des Körpers nennen. Der zyklische Kreisteilungskörper des Grades p^a, dessen einzige totalkritische Primzahl p ist, sei P_p; für $p = 2$ werde der reelle Körper dieser Art so bezeichnet. Daraus wird dann auch die Bezeichnung P_q erklärt; wir haben im dritten Abschnitt gesehen, daß $q-1$

durch p^a teilbar sein muß. Zyklische Körper desselben Grades nennen wir kurz „zugehörige Körper". Dann können wir den zweiten Hilfssatz so aussprechen:

Hat der zyklische Körper A_1 des Grades p^a die totalkritische Primzahl q, so ist das Produkt von A_1 und dem zugehörigen Körper P_q immer auch das Produkt von P_q und einem Abelschen Körper von nicht höherem Grade, dessen Diskriminante nicht durch q teilbar ist.

Aus A_1 und P_q entspringt der *Abel*sche Körper A, dessen Grad p^{a+b} ist, wo $b \leqq a$ ist. Da der Grad nicht durch q teilbar ist, so ist die Verzweigungsgruppe von q gleich E, und die Trägheitsgruppe von q ist deshalb eine zyklische Gruppe $\mathfrak{T}$. In dem Beweise zum ersten Hilfssatze war gezeigt worden, daß die Gruppe von A zyklische Untergruppen höchstens von der Ordnung p^a haben kann. Der Trägheitskörper von q hat deshalb mindestens den Grad p^b. Da aber seine Diskriminante nicht durch q teilbar ist, so ist er zu P_q teilerfremd; das Produkt beider hat mindestens den Grad p^{a+b}, also als Teiler von A genau diesen Grad. Deshalb hat der Trägheitskörper von q genau den Grad p^b, und A ist das Produkt von P_q und diesem Trägheitskörper, der die im Hilfssatze verlangten Eigenschaften hat.

6. *Der allgemeine Abelsche Körper.*

Zu Anfang des vorigen Abschnittes wurde bemerkt, daß jeder *Abel*sche Körper das Produkt von teilerfremden zyklischen Körpern ist, deren Grade Primzahlpotenzen sind. Nur für solche Körper braucht daher der Beweis erbracht zu werden. Von ihnen handeln die soeben abgeleiteten Hilfssätze, die wir zusammenfassen können in dem Satz: *Jeder zyklische Körper des Grades p^a kommt in einem Abelschen Körper als Teiler vor, der aus einem Kreisteilungskörper und einem Abelschen Körper einfacherer Art gebildet werden kann.* Diesen letzten Körper will ich kurz den Ergänzungskörper nennen.

Hat nun A vom Grade p^a die totalkritische Primzahl q, so gibt es einen Ergänzungskörper, dessen Diskriminante nicht mehr durch q teilbar ist. Er kann wieder in teilerfremde zyklische Körper zerlegt werden, die in derselben Weise wie A behandelt werden können. Die Grade der Ergänzungskörper sind niemals größer als p^a. Schließlich geht aus diesem

Verfahren ein Ergänzungskörper hervor, in dem nur noch p totalkritische Primzahl sein kann. Auf ihn, bzw. auf seine zyklischen Teiler wird nun der erste Hilfssatz angewandt. Es ergibt sich dabei ein Ergänzungskörper, dessen Grad kleiner als p^a ist: Denn wenn A nur die totalkritische Primzahl p hat, so hat sein Teiler p-ten Grades eine nur durch p teilbare Diskriminante, ist also ein Kreisteilungskörper, und A hat mit dem zugehörigen Körper P_p einen gemeinsamen Teiler. Der Fall $p=2$ macht hier keine Ausnahme, denn für $a>1$ hat A einen reellen Teiler zweiten Grades; für $a=1$ dagegen brauchen wir den ersten Hilfssatz nicht, der zweite allein führt auf lauter Kreisteilungskörper.

Die zyklischen Körper des Grades $p^{a'}$, $a'<a$ werden nun in derselben Weise weiter behandelt; schließlich muß das Verfahren auf Körper p-ten Grades führen, die sämtlich Kreisteilungskörper sind, wenn es nicht schon vorher aus demselben Grunde abgebrochen werden konnte. In dem Produkt aller benutzten Kreisteilungskörper ist dann der gegebene *Abel*sche Körper als Teiler enthalten.

Lebenslauf.

Ich, *Friedrich Steinbacher*, wurde am 4. Juni 1877 zu Berlin geboren und bin evangelischer Konfession. Zuletzt besuchte ich die Friedrichs-Werdersche Oberrealschule zu Berlin, an der ich Michaelis 1897 das Zeugnis der Reife erhielt. Michaelis 1899 bestand ich die Ergänzungsprüfung im Lateinischen am Falk-Realgymnasium. Von Michaelis 1897 bis Michaelis 1901 lag ich an der Universität Berlin besonders mathematischen Studien ob und hörte die Vorlesungen der Herren Professoren:

†*Dames*, *Dilthey*, *Förster*, *Frobenius*, †*Fuchs*, *Hensel*, *Hettner*, *Karsch*, *Knoblauch*, *Krigar-Menzel*, *Münch*, †*Paulsen*, *Planck*, *Plate*, †*Schaudinn*, *E. Schmidt*, *F. E. Schulze*, *Schumann*, *H. A. Schwarz*, *Schwendener*, †*Seeliger*, *Stumpf*, *Warburg*.

Dem mathematischen Seminar gehörte ich vier Semester an; an den von Herrn Prof. *Schwarz* geleiteten mathematischen Kolloquien nahm ich drei Semester lang teil. Außerdem beteiligte ich mich an den von Herrn Prof. *Planck* veranstalteten mathematisch-physikalischen Übungen und den Übungen zur Experimentalphysik unter Leitung von Herrn Prof. *Blasius*.

Im November 1902 bestand ich die Prüfung für das Lehramt an höheren Schulen; seit Michaelis 1904 bin ich Oberlehrer am Realgymnasium zu Friedrichshagen. Die Promotionsprüfung habe ich am 26. Mai 1910 bestanden.

Allen meinen hochverehrten Lehrern, besonders aber den Herren Geheimräten *Frobenius*, *H. A. Schwarz* und *Hensel* fühle ich mich zu großem Danke verpflichtet.